IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant:	Carpenter et al.		
Assignee:	Maxtor Corporation		
Title:	EXTREMELY SECURE METHOD FOR KEYING STORED CONTENTS TO A SPECIFIC STORAGE DEVICE		
Serial No.:	09/631,270	Filed:	August 2, 2000
Examiner:	Nguyen, M.	Group Art Unit:	2137
Atty. Docket No.:	Q00-1000-US1		

Board of Patent Appeals and Interferences
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450

APPEAL BRIEF
(37 C.F.R. § 41.37)

This Appeal Brief is in furtherance of the Notice of Appeal filed on November 15, 2004.

Please charge the $330 fee for filing this Appeal Brief to Deposit Account No. 13-0016/Q00-1000-US1 and charge any underpayment or credit any overpayment to this Account.

The index of subject matter is as follows:

I. REAL PARTY IN INTEREST

The real party in interest in this appeal is Maxtor Corporation.

II. RELATED APPEALS AND INTERFERENCES

There are no other appeals or interferences that will directly affect or be directly affected by or have a bearing on the Board's decision in this appeal.

III. STATUS OF CLAIMS

A. Total Number of Claims in Application

Claims in the application are: 1-110

B. Status of All Claims

1.	Claims canceled:	NONE
2.	Claims withdrawn:	NONE
3.	Claims pending:	1-110
4.	Claims allowed:	NONE
5.	Claims objected to:	13, 15, 17, 19 and 21
6.	Claims rejected:	1-12, 14, 16, 18, 20 and 22-110

C. Claims on Appeal

Claims on appeal are: 1-7, 12 and 22-110

IV. STATUS OF AMENDMENTS

No amendment has been filed after the outstanding Office Action dated May 19, 2004.

V. SUMMARY OF CLAIMED SUBJECT MATTER

Claim 1

The claimed subject matter is an extremely secure method for keying source content from a host processor to a source storage medium to prevent use of unauthorized copies of the source content. (Specification, page 3, lines 9-10 and page 5, lines 14-15).

The host processor reads a physical attribute of the source storage medium. The physical attribute is called the "source fingerprint." (Specification, page 3, lines 18-19 and page 5, lines 17-19 and Fig. 2A, step 104).

The host processor then merges (or combines) the physical attribute and the source content. The combined source content and source fingerprint is called the "fingerprinted content." (Specification, page 3, lines 18-19 and page 5, lines 19-21 and Fig. 2A, step 106).

The host processor then instructs the source storage medium to store the fingerprinted content. (Specification, page 5, lines 22-23 and Fig. 2A, step 108).

Claim 22[1]

The claimed subject matter is a method of securing source content from a hard disk drive (Specification, page 5, lines 14-17). The method includes:

(1) providing a source content in a host processor (Specification, page 5, lines 14-17);

[1] Claims 22-110 are rejected under 35 U.S.C. § 112, first paragraph, on the same basis and stand and fall together. Claim 22 illustrates the issues on appeal, so the summary of independent claims 51, 61 and 71 is omitted.

(2) providing a source fingerprint of a hard disk drive, wherein the source fingerprint is a physical attribute of the hard disk drive (Specification, page 4, lines 19-26 and page 5, lines 9-12);

(3) transferring the source fingerprint from the hard disk drive to the host processor (Specification, page 5, lines 17-19 and Fig. 2A, step 104); then

(4) generating a fingerprinted source content in the host processor using the source content and the source fingerprint, wherein the fingerprinted source content represents the source content and the source fingerprint (Specification, page 5, lines 19-21 and Fig. 2A, step 106); then

(5) transferring the fingerprinted source content from the host processor to the hard disk drive (Specification, page 5, lines 22-23 and Fig. 2A, step 108);

(6) storing the fingerprinted source content in the hard disk drive (Specification, page 5, lines 22-23 and Fig. 2A, step 108); then

(7) retransferring the fingerprinted source content from the hard disk drive to the host processor (Specification, page 5, lines 23-25 and Fig. 2B, step 112);

(8) generating the source content and the source fingerprint from the retransferred fingerprinted source content in the host processor (Specification, page 5, lines 25-26 and Fig. 2B, step 114);

(9) retransferring the source fingerprint from the hard disk drive to the host processor (Specification, page 5, lines 26-27 and Fig. 2B, step 116); and then

(10) comparing the generated source fingerprint with the retransferred source fingerprint in the host processor, wherein the host processor determines whether the generated source content is sanctioned in response to the comparison (Specification, page 5, lines 27-29 and Fig. 2B, steps 118 and 120).

VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

The grounds of rejection to be reviewed on appeal are (1) whether claims 22-110 should be rejected under 35 U.S.C. § 112, first paragraph, as containing subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the art that the inventors at the time the application was filed had possession of the claimed invention, and (2) whether claims 1-7 and 12 are unpatentable under 35 U.S.C. § 103(a) over *Stebbings* (U.S. Patent 6,684,199) in view of *Aucsmith* (U.S. Patent 6,148,407).

VII. ARGUMENT

I. SECTION 112, FIRST PARAGRAPH REJECTIONS

Claims 22-110 are rejected under 35 U.S.C. § 112, first paragraph, as containing subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the art that the inventors at the time the application was filed had possession of the claimed invention.

The Examiner asserts that "retransferring the fingerprinted . . ."; "generating the source content . . ." and "retransferring the source . . ." are not properly described in the application.

Independent claims 22, 51, 61 and 71 recite this terminology. Therefore, claim 22 is discussed below and separate discussion of claims 51, 61 and 71 is unnecessary. In other words, claims 22-110 stand and fall together.

Claim 22 recites this terminology at subparagraphs (7), (8) and (9) discussed above under SUMMARY OF CLAIMED SUBJECT MATTER.

In the Specification, Fig. 2B illustrates a generalized flowchart of extremely secure method 100 for reading and verifying fingerprinted contents of stored information (Specification, page 5, lines 14-17), and Fig. 4 illustrates in greater detail a generalized method 110 of reading and authenticating a source content method of Fig. 2B (Specification, page 6, lines 26-27).

Retransferring the Fingerprinted . . .

The subparagraph is "retransferring the fingerprinted source content from the hard disk drive to the host processor."

The Specification illustrates this feature in Fig. 2B, step 112 as follows:

> During a "reading and verifying fingerprinted contents" operation 110, in step 112 the host processor 16 commands the disk drive processor 22 to read fingerprinted content. (Specification, page 5, lines 23-25 (as amended in the Response dated March 8, 2004)).

The Specification also illustrates this feature in Fig. 4, step 112 as follows:

> In this example, generalized method 110 of reading and verifying fingerprinted content comprises a first step 112 of a host processor 16 commanding storage device 20 to read fingerprinted content. For convenience of illustration, we assume processor used in this example is host processor 16. However, it is envisioned that the processor or host referred to and used herein to implement method 110 of reading and verifying source content can be generally a processor in any host system coupled to a storage device 20. (Specification, page 6, line 27 to page 7, line 4 (as amended in the Response dated March 8, 2004)).

Thus, the Specification makes abundantly clear that at step 112, the fingerprinted content is transferred from storage device 20 to host processor 16. Moreover, since the fingerprinted content was previously transferred from host processor 16 to storage device 20 at step 108, it is perfectly appropriate to recite "retransferring" the fingerprinted content (or "fingerprinted source content") at step 112.

Claim 2 (original) also illustrates this feature:

> The extremely secure method of Claim 1 further comprising the step of a processor reading and verifying the fingerprinted content, the reading and verifying step comprising the steps of:
> instructing a local storage medium to read the fingerprinted content. (Claim 2, lines 1-4).

Claim 2 depends from claim 1, which recites "the host processor storing a fingerprinted content" and "instructing the source medium to store the fingerprinted content."

Thus, claim 2 makes abundantly clear that the fingerprinted content is transferred from the storage medium to the host processor. Moreover, since the storage medium was previously instructed to store the fingerprinted content, it is perfectly appropriate to recite "retransferring" the fingerprinted content (or "fingerprinted source content") from the storage medium back to the host processor at this later stage.

Generating the Source Content . . .

The subparagraph is "generating the source content and the source fingerprint from the retransferred fingerprinted source content in the host processor."

The Specification illustrates this feature in Fig. 2B, step 114 as follows:

> In step 114, host processor 16 separates content and fingerprint. (Specification, page 5, lines 25-26).

The Specification also illustrates this feature in Fig. 4, step 114 as follows:

> Method 110 further comprises step 114 wherein host processor 16 separates file contents to retrieve the fingerprint content. (Specification, page 7, lines 4-6 (as amended in the Response dated March 8, 2004)).

Thus, the Specification makes abundantly clear that at step 114, host processor 16 generates the source content and the source fingerprint from the fingerprinted content. Moreover, since the fingerprinted content was previously transferred from host processor 16 to storage device 20 at step 108, it is perfectly appropriate to recite the "retransferred" fingerprinted content (or "fingerprinted source content") at step 114.

Claim 2 (original) also illustrates this feature:

> The extremely secure method of Claim 1 further comprising the step of a processor reading and verifying the fingerprinted content, the reading and verifying step comprising the steps of: . . .
> separating the content to be secured from the source fingerprint. (Claim 2, lines 1-3 and 5).

Thus, claim 2 makes abundantly clear that the host processor separates the source content from the source fingerprint using the fingerprinted content read from the storage medium. Moreover, since the storage medium was previously instructed to store the fingerprinted content, it is perfectly appropriate to recite the "retransferred" fingerprinted content (or "fingerprinted source content") at this later stage.

Retransferring the Source . . .

The subparagraph is "retransferring the source fingerprint from the hard disk drive to the host processor."

The Specification illustrates this feature in Fig. 2B, step 116 as follows:

> Subsequently, in step 116, host processor 16 requests current storage device 20 to provide fingerprint information. (Specification, page 5, lines 26-27 (as amended in the Response dated March 8, 2004)).

The Specification also illustrates this feature in Fig. 4, step 116 as follows:

> Subsequently, in step 116, host processor 16 requests current storage device 20 to provide fingerprint information. (Specification, page 7, lines 6-7 (as amended in the Response dated March 8, 2004)).

Thus, the Specification makes abundantly clear that at step 116, the source fingerprint is transferred from storage device 20 to host processor 16. Moreover, since the source fingerprint was previously transferred from storage device 20 to host processor 16 at step 104, it is perfectly appropriate to recite "retransferring" the source fingerprint at step 116.

Claim 2 (original) also illustrates this feature:

> The extremely secure method of Claim 1 further comprising the step of a processor reading and verifying the fingerprinted content, the reading and verifying step comprising the steps of: . . .
>
> requesting a local fingerprint from the local medium (Claim 2, lines 1-3 and 6).

Thus, claim 2 makes abundantly clear that the source fingerprint is transferred from the storage medium to the host processor. Moreover, since the source fingerprint was previously determined from the storage medium, it is perfectly appropriate to recite "retransferring" the source fingerprint from the storage medium to the host processor at this later stage.

The M.P.E.P. discusses the written description requirement as follows:

> To satisfy the written description requirement, a patent specification must describe the claimed invention in sufficient detail that one skilled in the art can reasonably conclude that the inventor had possession of the claimed invention. (M.P.E.P. § 2163(I), Rev. 2, May 2004, page 2100-164.)
>
> An applicant shows possession of the claimed invention by describing the claimed invention with all of its limitations using such descriptive means as words, structures, figures, diagrams, and formulas that fully set forth the claimed invention. (M.P.E.P. § 2163(I), Rev. 2, May 2004, page 2100-165.)
>
> The claims as filed in the original specification as part of the disclosure . . . (M.P.E.P. § 2163(I)(B), Rev. 2, May 2004, page 2100-167.)
>
> While there is no *in haec verba* requirement, newly added claim limitations must be supported in the specification through express, implicit, or inherent disclosure. (M.P.E.P. § 2163(I)(B), Rev. 2, May 2004, page 2100-167.)
>
> The Examiner, therefore, must have a reasonable basis to challenge the adequacy of the written description requirement. The examiner has the initial burden of presenting by a preponderance of evidence why a person skilled in the art would not recognize in an applicant's disclosure a description of the invention defined by the claims. (M.P.E.P. § 2163.04, Rev. 2, May 2004, page 2100-179.)

The Specification need only describe the claimed invention in sufficient detail that one skilled in the art can reasonably conclude that the inventor had possession of the claimed invention. Furthermore, the Specification can describe the claimed invention using words and figures through express, implicit, or inherent disclosure. There is no *in haec verba* requirement.

Applicant has provided detailed explanations of how both the Specification and original claims describe the terminology mentioned above. These detailed explanations establish that the original disclosure describes this terminology in sufficient detail that one skilled in the art can reasonably conclude, indeed readily conclude, that the inventors had possession of the claimed subject matter.

The Examiner has the burden of presenting by a preponderance of evidence why a person skilled in the art would not recognize that the Specification reasonably conveys this terminology. Unfortunately, the Examiner has not even attempted to provide an explanation. Instead, the Examiner merely asserts that the terminology "are not properly described in the specification." Thus, the Examiner has no explanation whatsoever. Since the Examiner has failed to meet (over even attempt to meet) this burden, for this reason alone, the rejection is improper. Moreover, the rejection has no merit for the reasons discussed above. Therefore, the rejection is clearly erroneous both procedurally and substantively.

II. SECTION 103 REJECTIONS – STEBBINGS AND AUCSMITH

Claims 1-12, 14, 16, 18 and 20 are rejected under 35 U.S.C. § 103(a) as being unpatentable over *Stebbings* (U.S. Patent 6,684,199) in view of *Aucsmith* (U.S. Patent 6,148,407).

Stebbings discloses a method for preventing unauthorized copying of data. In the original storage device, predetermined errors that provide a decryption key are intentionally embedded in the data. The playback device includes a Reed-Solomon decoder that not only corrects the predetermined errors, but also removes the predetermined errors from the audio. As a result, the storage device is stripped of the necessary decryption key required for subsequent playback by another playback device.

Stebbings makes clear that the predetermined errors are devised independently of the storage device:

> In this embodiment, the data media is a CD 20 onto which predetermined errors are intentionally embedded. . . . These

> errors are mixed and edited with the original data before being burned into a master disc, which is replicated to produce a desired number of CDs. (Col. 20, lines 53-56).

Aucsmith discloses a method for computer platform identification.

Aucsmith considers a single component identifier (such as manufacturer, model, and/or performance traits) to be problematic:

> The use of any single component identifier (e.g., manufacturer, model, and/or performance traits) is problematic for a number of reasons. First, component identifiers, such as Ethernet addresses, are not universally available in every platform. Second, such component identifiers are generally not unique. For example, BIOS (Basic Input / Output Software) identifications are neither unique nor universally available. Additionally, the use of a single identifier, such as a central processing unit identification (CPUID) may prove problematic when the system is upgraded. Any such scheme relying on a single component identifier will fail if the component is replaced with a higher performance component as is routinely done in the process of upgrading. (Col. 1, lines 40-53).

Aucsmith solves this problem by generating a computer platform identification, or fingerprint, using a plurality of computer system traits. In this manner, the fingerprint provides a reasonably unique identification that accommodates platform upgrades occurring during the platform's lifetime.

The traits are characteristics, preferences, or qualities in the computer system which may or may not be subject to change through-out the life of the computer system. Traits include hardware attributes, such as manufacturer and performance characteristics, software versions, and user preferences. For instance, traits include the processor ID, the cache ID, the RAM size, the hard drive number and capacity of disks, the network card address, the modem ID and speed, the video card manufacturer, the CD ROM type, the operating system manufacturer and version, and preferences selected for use with the operating system or application programs.

Claim 1 recites "the source fingerprint is a physical attribute of the source storage medium." *Stebbings* fails to teach or suggest that the predetermined errors are a physical attribute of the storage device. *Aucsmith* fails to teach or suggest that the predetermined errors should be replaced by the platform identifier.

The predetermined errors, by definition, are predetermined, whereas the platform identifier is a unique fingerprint based on a plurality of traits. The predetermined errors are burned into a master disc, then stamped from the master disc onto the original CDs during volume manufacturing, and then removed from the original CDs during initial playback.

Aucsmith fails to teach or suggest that the predetermined errors burned into the master disc should be customized (a platform identifier) to reflect a physical attribute of each original CD being stamped, as this makes absolutely no sense. This would defeat the purpose of creating the master disc to stamp original CDs, and would be completely unnecessary since the original playback device removes the predetermined errors.

In sustaining the rejection, the Examiner states as follows:

> It would have been obvious to one of ordinary skill in the art at the time of the invention to employ the use of physical attribute of the storage medium as source fingerprint, as Aucsmith teaches, in the system of Stebbings so as to strengthen data security in the system.

The rejection is flawed for several reasons.

First, *Aucsmith* is non-analogous to the present invention. *Aucsmith* is directed to computer platform identification. The present invention, on the other hand, is directed to an extremely secure method of keying stored content to a specific storage device. In order to be analogous art, the reference must either be in the field of the invention or be reasonably pertinent to the particular problem with which the inventor was concerned (M.P.E.P. § 2141.01(a), Rev. 2, May 2004, page 2100-122). *Aucsmith* is neither within the field of the invention (data storage) nor pertinent to the particular problem with which the inventor was concerned (extremely secure data storage on a specific storage device to prevent unauthorized copying).

Second, *Aucsmith* fails to teach or suggest the proposed modification that the predetermined errors in *Stebbings* be replaced by the platform identifier in *Aucsmith*. The proposed modification would require a platform identifier that reflects a physical attribute of an individual CD be burned into the master disc used to stamp large quantities of original CDs. This would defeat the purpose the master disc, thereby rendering *Stebbings* unsatisfactory for its intended purpose.

Third, the Examiner has failed to explain how or why the proposed modification would "strengthen data security." *Stebbings* teaches an effective data security protection scheme in which the original playback device removes the predetermined errors, thereby preventing a subsequent playback device from functioning. Unique predetermined errors would serve no purpose since the subsequent playback device would never see them. The proposed modification would do nothing to enhance data security protection in *Stebbings*, and instead, would vastly complicate manufacturing without providing a benefit. Thus, the Examiner has failed to establish any motivation for the proposed modification.

Fourth, even if the proposed modification was made (although there is no teaching, suggestion or motivation to do so), the Examiner has failed to explain what traits in *Aucsmith* could be applied to uniquely identify an original CD (or data storage device) in *Stebbings*. *Aucsmith* lists numerous traits for a computer platform, however the listed traits for a data storage device (such as the number or capacity of disks) would fail to uniquely identify the data storage device.

To establish a prima facie case of obviousness (1) there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or combine reference teachings; (2) there must be a reasonable expectation of success; and (3) the prior art reference (or references when combined) must teach or suggest all the claim limitations (MPEP § 2143, Rev. 2, May 2004, page 2100-129). See also *C.R. Bard, Inc. v. M3 Systems, Inc.*, 157 F.3d 1340, 1351 (Fed. Cir. 1998).

It is insufficient that the prior art shows similar components unless it also contains some teaching, suggestion or incentive for arriving at the claimed structure. See *Northern Telecom, Inc. v. Datapoint Corp.*, 908 F.2d 931, 934 (Fed. Cir. 1990).

Moreover, if the proposed modification would render the prior art unsatisfactory for its intended purpose, then there is no suggestion or motivation to make the proposed modification (M.P.E.P. § 2143.01, Rev. 2, May 2004, page 2100-131).

Finally, non-analogous prior art cannot be used to sustain an obviousness rejection (M.P.E.P. § 2141.01(a), Rev. 2, May 2004, page 2100-122).

I hereby certify that this correspondence is being deposited with the United States Postal Service with sufficient postage as First Class Mail in an envelope addressed to: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450, on January 3, 2005.

D Sigmond — 1/3/05

David M. Sigmond
Attorney for Applicant

Date of Signature

Respectfully submitted,

D Sigmond

David M. Sigmond
Attorney for Applicant
Reg. No. 34,013
(303) 702-4132
(303) 678-3111 (fax)

VIII. CLAIMS APPENDIX

1. An extremely secure method for a host processor to key a source content to a source storage medium to prevent use of an unauthorized copy of the source content comprising the host processor storing a fingerprinted content comprising the steps of:

determining a source fingerprint from the source storage medium, wherein the source fingerprint is a physical attribute of the source storage medium;

combining the source content to be secured with the source fingerprint to generate the fingerprinted content; and

instructing the source storage medium to store the fingerprinted content.

2. The extremely secure method of Claim 1 further comprising the step of a host processor reading and verifying the fingerprinted content, the reading and verifying step comprising the steps of:

instructing a local storage medium to read the fingerprinted content;

separating the source content to be secured from the source fingerprint;

requesting a local fingerprint from the local storage medium; and

comparing the local fingerprint with the source fingerprint and in response to the comparison determining whether to use the source content.

3. The extremely secure method of Claim 2 wherein the step of determining a source fingerprint further comprises:

using an open protocol to request a secured communication from the source storage medium;

identifying a physical, statistically unique, verifiable and relatively immutable (PSUVI) characteristic associated with the source storage medium;

generating encryption and/or decryption keys;

returning the encryption key to the host processor;

using the encryption key to convert the source content to an encrypted protocol;

requesting from the source storage medium the PSUVI characteristic; and

the source storage medium responding to the host processor with the PSUVI characteristic.

4. The extremely secure method of Claim 2 wherein the step of combining the source content with the source fingerprint to generate the fingerprinted content further comprises:

creating a hybrid content to be secured by combining the source content to be secured and the source fingerprint; and

encrypting the fingerprinted content with an encryption key.

5. The extremely secure method of Claim 2 wherein the step of requesting a local fingerprint from the local storage medium further comprises the steps of:

requesting from the local storage storage medium a local PSUVI characteristic;

replying to the host processor with the local PSUVI characteristic; and

performing a secured verification of the local PSUVI characteristic.

6. The extremely secure method of Claim 2 wherein the step of determining a source fingerprint further comprises:

using an open protocol to request a secured communication from the source storage medium;

identifying a relatively mutable physical attribute (Non-PSUVI) characteristic associated with the source storage medium;

generating encryption and/or decryption keys;

returning the encryption key to the host processor;

using the encryption key to convert the source content to an encrypted protocol;

requesting from the source storage medium the non-PSUVI characteristic; and

the source storage medium responding to the host processor with the non-PSUVI characteristic.

7. The extremely secure method of Claim 2 wherein the step of requesting a local fingerprint from the local storage medium further comprises the steps of:

requesting from the local storage medium a local non-PSUVI characteristic;

replying to the host processor with the local non-PSUVI characteristic; and

performing a secured verification of the local non-PSUVI characteristic.

12. The extremely secure method of Claim 1, wherein the source storage medium is a hard disk drive.

22. A method of securing source content from a hard disk drive, comprising:

providing a source content in a host processor;

providing a source fingerprint of a hard disk drive, wherein the source fingerprint is a physical attribute of the hard disk drive;

transferring the source fingerprint from the hard disk drive to the host processor; then

generating a fingerprinted source content in the host processor using the source content and the source fingerprint, wherein the fingerprinted source content represents the source content and the source fingerprint; then

transferring the fingerprinted source content from the host processor to the hard disk drive;

storing the fingerprinted source content in the hard disk drive; then

retransferring the fingerprinted source content from the hard disk drive to the host processor;

generating the source content and the source fingerprint from the retransferred fingerprinted source content in the host processor;

retransferring the source fingerprint from the hard disk drive to the host processor; and then

comparing the generated source fingerprint with the retransferred source fingerprint in the host processor, wherein the host processor determines whether the generated source content is sanctioned in response to the comparison.

23. The method of Claim 22, wherein the source fingerprint is a statistically unique physical attribute of the hard disk drive.

24. The method of Claim 23, wherein the source fingerprint is a relatively immutable physical attribute of the hard disk drive.

25. The method of Claim 24, wherein the source fingerprint is a statistically unique, immutable and verifiable physical attribute of the hard disk drive.

26. The method of Claim 22, wherein the source fingerprint is a detect list of the hard disk drive.

27. The method of Claim 26, wherein the defect list includes physical block addresses.

28. The method of Claim 22, wherein the source fingerprint is a servo characteristic of the hard disk drive.

29. The method of Claim 28, wherein the servo characteristic is servo burst correction values.

30. The method of Claim 28, wherein the servo characteristic is servo burst correction value related repeatable runout response.

31. The method of Claim 28, wherein the servo characteristic is servo wedge defects.

32. The method of Claim 28, wherein the servo characteristic is a servo transfer function.

33. The method of Claim 22, wherein the source fingerprint is a track misregistration behavior of the hard disk drive.

34. The method of Claim 22, wherein the source fingerprint is a channel optimization of the hard disk drive.

35. The method of Claim 34, wherein the channel optimization is a read channel optimization parameter related to an individual head.

36. The method of Claim 34, wherein the channel optimization is a write channel optimization parameter related to an individual head.

37. The method of Claim 22, wherein the source fingerprint is a statistically unique physical property of a head disk assembly of the hard disk drive.

38. The method of Claim 22, wherein the source fingerprint is a statistically unique physical property of a printed circuit board of the hard disk drive.

39. The method of Claim 22, wherein the source fingerprint is magnetic defects of the hard disk drive.

40. The method of Claim 22, wherein the source fingerprint is a head/media characteristic of the hard disk drive.

41. The method of Claim 22, including transferring an encryption key from the hard disk drive to the host processor.

42. The method of Claim 41, wherein generating the fingerprinted source content includes generating an encrypted source content using the source content and the encryption key in the host processor, and then generating the fingerprinted source content using the encrypted source content and the source fingerprint in the host processor.

43. The method of Claim 41, wherein generating the fingerprinted source content includes generating a non-encrypted fingerprinted source content using the source content and the source fingerprint in the host processor, and then generating an encrypted fingerprinted source content using the non-encrypted fingerprinted source content and the encryption key.

44. The method of Claim 22, wherein generating the fingerprinted source content includes encrypting the source content and the source fingerprint using an encryption algorithm.

45. The method of Claim 22, wherein generating the source content includes decrypting the fingerprinted source content using a decryption algorithm.

46. The method of Claim 22, wherein comparing the generated source fingerprint with the retransferred source fingerprint includes determining whether the generated source fingerprint and the retransferred source fingerprint match using statistical analysis.

47. The method of Claim 46, wherein the statistical analysis includes determining whether a statistically large percentage of defects listed in the generated source fingerprint point to defects in the retransferred source fingerprint.

48. The method of Claim 46, wherein the statistical analysis includes determining whether a statistically small percentage of defects listed in the generated source fingerprint point to defects in the retransferred source fingerprint.

49. The method of Claim 22, wherein the generated source content is enabled for use by the host processor if the generated source fingerprint matches the retransferred source fingerprint, and the generated source content is disabled for use by the host processor if the generated source fingerprint does not match the retransferred source fingerprint.

50. The method of Claim 22, wherein the host processor uses the generated source content if the generated source fingerprint matches the retransferred source fingerprint, and the

host processor does not use the generated source content if the generated source fingerprint does not match the retransferred source fingerprint.

51. A method of securing source content from a hard disk drive, comprising:

providing a source content in a host processor;

providing a source fingerprint of a hard disk drive, wherein the source fingerprint is a physical, statistically unique, verifiable and relatively immutable (PSUVI) characteristic of the hard disk drive;

transferring the source fingerprint from the hard disk drive to the host processor; then

generating a fingerprinted source content in the host processor using the source content and the source fingerprint, wherein the fingerprinted source content represents the source content and the source fingerprint; then

transferring the fingerprinted source content from the host processor to the hard disk drive;

storing the fingerprinted source content in the hard disk drive; then

retransferring the fingerprinted source content from the hard disk drive to the host processor;

generating the source content and the source fingerprint from the retransferred fingerprinted source content in the host processor;

retransferring the source fingerprint from the hard disk drive to the host processor; and then

comparing the generated source fingerprint with the retransferred source fingerprint in the host processor, wherein the host processor determines whether the generated source content is sanctioned in response to the comparison.

52. The method of Claim 51, wherein the source fingerprint is an immutable characteristic of the hard disk drive.

53. The method of Claim 51, wherein the source fingerprint is a defect list.

54. The method of Claim 51, including transferring an encryption key from the hard disk drive to the host processor.

55. The method of Claim 54, wherein generating the fingerprinted source content includes generating an encrypted source content using the source content and the encryption key in the host processor, and then generating the fingerprinted source content using the encrypted source content and the source fingerprint in the host processor.

56. The method of Claim 54, wherein generating the fingerprinted source content includes generating a non-encrypted fingerprinted source content using the source content and the source fingerprint in the host processor, and then generating an encrypted fingerprinted source content using the non-encrypted fingerprinted source content and the encryption key.

57. The method of Claim 51, wherein generating the fingerprinted source content includes encrypting the source content and the source fingerprint using an encryption algorithm.

58. The method of Claim 51, wherein generating the source content includes decrypting the fingerprinted source content using a decryption algorithm.

59. The method of Claim 51, wherein the generated source content is enabled for use by the host processor if the generated source fingerprint matches the retransferred source fingerprint, and the generated source content is disabled for use by the host processor if the generated source fingerprint does not match the retransferred source fingerprint.

60. The method of Claim 51, wherein the host processor uses the generated source content if the generated source fingerprint matches the retransferred source fingerprint, and the host processor does not use the generated source content if the generated source fingerprint does not match the retransferred source fingerprint.

61. A method of securing source content from a hard disk drive, comprising:

providing a source content in a host processor;

providing a media detect list of the hard disk drive;

transferring the media defect list from the hard disk drive to the host processor; then

generating a fingerprinted source content in the host processor using the source content and the media defect list, wherein the fingerprinted source content represents the source content and the source fingerprint; then

transferring the fingerprinted source content from the host processor to the hard disk drive;

storing the fingerprinted source content in the hard disk drive; then

retransferring the fingerprinted source content from the hard disk drive to the host processor;

generating the source content and the media detect list from the retransferred fingerprinted source content in the host processor;

retransferring the media defect list from the hard disk drive to the host processor; and then

comparing the generated media defect list with the retransferred media defect list in the host processor, wherein the host processor determines whether the generated source content is sanctioned in response to the comparison.

62. The method of Claim 61, wherein the media defect list is a statistically unique, immutable and verifiable physical attribute of the hard disk drive.

63. The method of Claim 61, wherein the media defect list includes physical block addresses.

64. The method of Claim 61, including transferring an encryption key from the hard disk drive to the host processor.

65. The method of Claim 64, wherein generating the fingerprinted source content includes generating an encrypted source content using the source content and the encryption key

in the host processor, and then generating the fingerprinted source content using the encrypted source content and the media defect list in the host processor.

66. The method of Claim 64, wherein generating the fingerprinted source content includes generating a non-encrypted fingerprinted source content using the source content and the media defect list in the host processor, and then generating an encrypted fingerprinted source content using the non-encrypted fingerprinted source content and the encryption key.

67. The method of Claim 61, wherein generating the fingerprinted source content includes encrypting the source content and the media defect list using an encryption algorithm.

68. The method of Claim 61, wherein generating the source content includes decrypting the fingerprinted source content using a decryption algorithm.

69. The method of Claim 61, wherein the generated source content is enabled for use by the host processor if the generated media defect list matches the retransferred media defect list, and the generated source content is disabled for use by the host processor if the generated media defect list does not match the retransferred media defect list.

70. The method of Claim 61, wherein the host processor uses the generated source content if the generated media defect list matches the retransferred media defect list, and the host processor does not use the generated source content if the generated media defect list does not match the retransferred media defect list.

71. A method of securing source content from a hard disk drive, comprising:

providing a source content in a host processor;

providing a first source fingerprint of a first hard disk drive, wherein the first source fingerprint is a physical, statistically unique, verifiable and relatively immutable (PSUVI) characteristic of the first hard disk drive;

providing a second source fingerprint of a second hard disk drive, wherein the second source fingerprint is a physical, statistically unique, verifiable and relatively immutable (PSUVI) characteristic of the second hard disk drive;

transferring the first source fingerprint from the first hard disk drive to the host processor;

generating a fingerprinted source content in the host processor using the source content and the first source fingerprint, wherein the fingerprinted source content represents the source content and the first source fingerprint; then

transferring the fingerprinted source content from the host processor to a selected hard disk drive;

storing the fingerprinted source content in the selected hard disk drive; then

retransferring the fingerprinted source content from the selected hard disk drive to a host device;

generating the source content and the first source fingerprint from the retransferred fingerprinted source content in the host device;

transferring a selected source fingerprint from the selected hard disk drive to the host device, wherein the selected source fingerprint is the first source fingerprint if the selected hard disk drive is the first hard disk drive, and the selected source fingerprint is the second source fingerprint if the selected hard disk drive is the second hard disk drive; and then

comparing the generated source fingerprint with the selected source fingerprint in the host device, wherein the host device determines that the generated source content is sanctioned if the generated source fingerprint matches the selected source fingerprint, and the host device determines that the generated source content is unsanctioned if the generated source fingerprint does not match the selected source fingerprint.

72. The method of Claim 71, wherein the first source fingerprint is an immutable characteristic of the first hard disk drive, and the second source fingerprint is an immutable characteristic of the second hard disk drive.

73. The method of Claim 71, wherein the first source fingerprint is a first detect list of the first hard disk drive, and the second source fingerprint is a second detect list of the second hard disk drive.

74. The method of Claim 73, wherein the first defect list includes first physical block addresses, and the second defect list includes second physical block addresses.

75. The method of Claim 71, wherein the first source fingerprint is a first servo characteristic of the first hard disk drive, and the second source fingerprint is a second servo characteristic of the second hard disk drive.

76. The method of Claim 75, wherein the first servo characteristic is first servo burst correction values, and the second servo characteristic is second servo burst correction values.

77. The method of Claim 75, wherein the first servo characteristic is first servo burst correction value related repeatable runout response, and the second servo characteristic is second servo burst correction value related repeatable runout response.

78. The method of Claim 75, wherein the first servo characteristic is first servo wedge defects, and the second servo characteristic is second servo wedge defects.

79. The method of Claim 75, wherein the first servo characteristic is a first servo transfer function, and the second servo characteristic is a second servo transfer function.

80. The method of Claim 71, wherein the first source fingerprint is a track misregistration behavior of the first hard disk drive, and the second source fingerprint is a track misregistration behavior of the second hard disk drive.

81. The method of Claim 71, wherein the first source fingerprint is a first channel optimization of the first hard disk drive, and the second source fingerprint is a second channel optimization of the second hard disk drive.

82. The method of Claim 81, wherein the first channel optimization is a read channel optimization parameter related to a first individual head, and the second channel optimization is a read channel optimization parameter related to a second individual head.

83. The method of Claim 81, wherein the first channel optimization is a write channel optimization parameter related to a first individual head, and the second channel optimization is a write channel optimization parameter related to a second individual head.

84. The method of Claim 71, wherein the first source fingerprint is a statistically unique physical property of a head disk assembly of the first hard disk drive, and the second source fingerprint is a statistically unique physical property of a head disk assembly of the second hard disk drive.

85. The method of Claim 71, wherein the first source fingerprint is a statistically unique physical property of a printed circuit board of the first hard disk drive, and the second source fingerprint is a statistically unique physical property of a printed circuit board of the second hard disk drive.

86. The method of Claim 71, wherein the first source fingerprint is magnetic defects of the first hard disk drive, and the second source fingerprint is magnetic defects of the second hard disk drive.

87. The method of Claim 71, wherein the first source fingerprint is a head/media characteristic of the first hard disk drive, and the second source fingerprint is a head/media characteristic of the second hard disk drive.

88. The method of Claim 71, including transferring an encryption key from the first hard disk drive to the host processor.

89. The method of Claim 88, wherein generating the fingerprinted source content includes generating an encrypted source content using the source content and the encryption key in the host processor, and then generating the fingerprinted source content using the encrypted source content and the first source fingerprint in the host processor.

90. The method of Claim 88, wherein generating the fingerprinted source content includes generating a non-encrypted fingerprinted source content using the source content and the first source fingerprint in the host processor, and then generating an encrypted fingerprinted source content using the non-encrypted fingerprinted source content and the encryption key.

91. The method of Claim 71, wherein generating the fingerprinted source content includes encrypting the source content and the first source fingerprint using an encryption algorithm.

92. The method of Claim 71, wherein generating the source content includes decrypting the fingerprinted source content using a decryption algorithm.

93. The method of Claim 71, wherein the selected hard disk drive is the first hard disk drive, the selected source fingerprint is the first source fingerprint, and the host device determines that the generated source content is sanctioned.

94. The method of Claim 93, wherein the host device is the host processor.

95. The method of Claim 71, wherein the selected hard disk drive is the second hard disk drive, the selected source fingerprint is the second source fingerprint, and the host device determines that the generated source content is unsanctioned.

96. The method of Claim 95, wherein the host device is another processor.

97. The method of Claim 95, wherein transferring the fingerprinted source content from the host processor to the second hard disk drive includes transferring the fingerprinted source content from the host processor to the first hard disk drive, and then transferring the fingerprinted source content from the first hard disk drive to the second hard disk drive.

98. The method of Claim 97, wherein transferring the fingerprinted source content from the first hard disk drive to the second hard disk drive includes transferring a drive image copy of the fingerprinted source content from the first hard disk drive to the second hard disk drive.

99. The method of Claim 97, wherein transferring the fingerprinted source content from the first hard disk drive to the second hard disk drive is performed using low-level block copy software.

100. The method of Claim 97, wherein the host device is another processor.

101. The method of Claim 71, wherein the host device is the host processor.

102. The method of Claim 71, wherein the host device is another processor.

103. The method of Claim 71, wherein comparing the generated source fingerprint with the selected source fingerprint includes determining whether the generated source fingerprint and the selected source fingerprint match using statistical analysis.

104. The method of Claim 103, wherein the statistical analysis includes determining whether a statistically large percentage of items listed in the generated source fingerprint are consistent with the selected source fingerprint.

105. The method of Claim 103, wherein the statistical analysis includes determining whether a statistically small percentage of items listed in the generated source fingerprint are inconsistent with the selected source fingerprint.

106. The method of Claim 103, wherein the statistical analysis includes determining whether a statistically large percentage of defects listed in the generated source fingerprint point to defects in the selected source fingerprint.

107. The method of Claim 103, wherein the statistical analysis includes determining whether a statistically small percentage of defects listed in the generated source fingerprint point to defects in the selected source fingerprint.

108. The method of Claim 71, wherein the generated source content is enabled for use by the host device if the generated source fingerprint matches the selected source fingerprint, and the generated source content is disabled for use by the host device if the generated source fingerprint does not match the selected source fingerprint.

109. The method of Claim 71, wherein the host device uses the generated source content if the generated source fingerprint matches the selected source fingerprint, and the host device does not use the generated source content if the generated source fingerprint does not match the selected source fingerprint.

110. The method of Claim 71, wherein the host device determines that the generated source content is an authorized copy of the source content if the generated source fingerprint matches the selected source fingerprint, and the host device determines that the generated source content is an unauthorized copy of the source content if the generated source fingerprint does not match the selected source fingerprint.